AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☑ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
information related to the Google accounts associated with the following telephone number and/or email addresses, all of which are stored at premises controlled by Google, Inc. ("Google" or "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043: i. 815-408-0854; ii. quinnblackbukateferguson1820@gmail.com; iii. loganclarketour@gmail.com

Case No. 24-871M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 7/4/2024 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/20/2024 @ 4:31 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information related to the Google accounts associated with the following telephone number and/or email addresses, all of which are stored at premises controlled by Google, Inc. ("Google" or "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043**:**

i. 815-408-0854

ii. quinnblackbukateferguson1820@gmail.com

iii. loganclarketour@gmail.com

.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period April 20, 2024 through April 29, 2024:

1. Subscriber/registration information to include name, emails, phone numbers, addresses, account creation dates, account status, registration IP address, means and source of payment (including any credit or bank account numbers);

2. Device identifiers (IMEI/MEID, serial number, SIM operator, cell operator, and model number, etc.), account identifiers, Android ID, Push Tokens and/or Device Tokens, etc. associated with the Account(s);

3. All IP Address logs for all services utilized by the Account(s), to include records of session times and durations, login/logout/intra-communication IP addresses associated with session times and date, methods of connecting, and log files;

4. Location history for all identified/associated Account(s), to include deleted information, derived from Global Positioning System (GPS) data, cell site/cell tower triangulation precision measurement information such as timing advance or per call measurement data, Wi-Fi location information, and Bluetooth location information. Such data shall include the GPS coordinates, the dates and times of all location recordings, origin of how the location recordings were obtained, and estimated radius;

5. All Gmail address(es) associated with the identified Account(s) including any secondary or backup email addresses associated with the Accounts;

6. The contents of all text messages, voicemails, recorded calls, emails chat messages, and saved drafts associated with the Account(s), including stored/preserved copies and contents maintained on a cloud service, the source and destination addresses associated with each communication, the date and time at which each communication was sent, and the size/length/duration of each communication;

7. All photos and videos stored in the Account(s);

8. Passwords or other protective devices in place and associated with the Account(s), which would permit access to the content stored therein;

9. Web search history, including, but not limited to, mobile and desktop browser searches;

10. Downloaded, installed, and/or purchased apps along with activity/registration information;

11. Voice and/or audio activity recordings/captures;

12. Google Map locations which are saved and/or frequent locations, favorite and/or starred locations including, but not limited to, searches conducted using the Google Map and/or Maze services;

13. Google Voice incoming or outgoing phone calls, voicemails, including voicemail content and any and all incoming or outgoing text message history, together with the content thereof to include SMS, MMS, or any other form of text message communication, and any call forwarding numbers and account backup telephone numbers;

14. Communication including, but not limited to, audio, video, text message and/or chat delivered through the Google, Inc. service known as Google Hangouts;

15. Posts, status updates, photographs and/or videos that are contained and/or were uploaded in the services known as Google Photos, Picasa web albums, Google +, or any other service designed to store video, photographs, and/or data, including the metadata for each file;

16. Electronic files, folders, media, and/or data uploaded and/or contained on the service known as Google Drive;

17. Entries created, deleted, or modified using the service known as Google Keep;

18. Contacts stored using the service known as Google Contacts, including any contacts stored in the service known as Gmail, and any other service where contact lists are maintained;

19. Google Play Store transactions;

20. Additional accounts linked by cookies.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 875, interstate communication with intent to extort.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information related to the Google accounts associated with the following telephone number and/or email addresses, all of which are stored at premises controlled by Google, Inc. ("Google" or "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043: i. 815-408-0854; ii. quinnblackbukateferguson1820@gmail.com; iii. loganclarketour@gmail.com

Case No. 24-871M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 875	interstate communication with threats to injure and/or extort

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Heather Wright, Special Agent - FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 6/20/2024

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS

I, Heather N. Wright, being first duly sworn on oath, on information and belief state:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since July of 2010. Since August of 2020, I have been assigned to the FBI's Milwaukee Area Violent Crimes Task Force, a multi-jurisdictional law enforcement entity charged with investigating violations of federal law, including bank robberies, commercial robberies, armed motor vehicle robberies, and other violent crime matters, defined under Title 18 of the United States Code. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

2. I make this affidavit in support of applications for search warrants for the following information that is controlled and maintained by Google, Inc. ("Google"), which is headquartered at 1600 Amphitheatre Parkway, Mountain View, California:

a. Information related to the accounts associated with a telephone number 815-408-0854, and/or email addresses loganclarketour@gmail.com, quinnblackbukateferguson1820@gmail.com, which are associated to an unknown subject responsible for violations of Title 18, United States Code, Section 875 (interstate communication with threats to injure and/or extort). This account is further described in the following paragraphs and in Attachment A. The information to be disclosed by Google

is described in Section I of Attachment B while the information to be seized by the government is described in Section II of Attachment B.

3. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 875 have been committed, are being committed, and will be committed by unknown actors this warrant is sought after to identify. There is also probable cause to search for the information described Attachment B associated with the accounts described in Attachment A for evidence, fruits, and instrumentalities of these crimes.

4. The statements in this affidavit are based upon my investigation, information provided by other law enforcement officers, and on my experience and training as a Special Agent of the FBI. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of the violations of federal law committed by the account holders listed in Attachment A are located in the contents of specified Google accounts.

PROBABLE CAUSE

5. On April 24, 2024, at 8:37 p.m., the Kenosha Police Department responded to a bomb threat that was called into the non-emergency line from the Google Voice number 815-408-0854. The caller stated that he had left three pipe bombs inside a bathroom stall within the Little Learner's Child Development Center located at 4212 52nd Street in Kenosha, Wisconsin. The caller stated that a female employee had let him into the building to use the bathroom where he was able to place the bombs with a twenty-minute timer. The caller made a statement that he wanted the building and the children inside to explode. The caller remained on the phone and advised that he was in a red Toyota Camry on 43rd Avenue watching the business and could see a police car. Upon

arriving on scene, officers made contact with the business, noting that the doors were locked and there were no lights on. Officers did not observe any vehicles in the parking lot of the business aside from a red van associated to the business. Officers checked the rear (north) door for the business and it was also secured. The business hours listed showed that it was to close at 7:00 p.m. Dispatch attempted to make contact with the owner but was unsuccessful.

6. While checking the building, officers observed an occupied red Toyota Corolla in the parking lot for U-Haul Moving and Storage, located nearby at 4404 52nd Street. Officers approached the vehicle and made contact with the driver. The driver appeared to be sleeping and was questioned by police. The driver advised that he was at the business to pay for his storage unit. The driver was cooperative and provided his telephone number to officers, which did not match the number used to call in the threat. Dispatch called the number provided and spoke to the driver in the presence of officers. The driver also consented to have officers view the call log within his phone. Officers were able to confirm that no calls to the Kenosha Police Department non-emergency line were logged. The driver was released after confirming that he had no connection to the called threat.

7. After this incident was reported to EGuardian and the recorded into the FBI's complaint database, it was determined that several additional false emergency response requests had been reported on April 24, 2024 and April 25, 2024. I noted that on April 24, 2024, at approximately 5:33 p.m. PDT (7:33 p.m. CST), a bomb threat was reported to the San Jose Police Department dispatch. The reporting party identified themselves as DYLAN JESSUP and called from telephone number 815-408-0854. The subject stated that the bomb was located inside a black Adidas sports duffel bag within the bathroom of the San Jose City College, located at 2100 Moorpark Avenue in San Jose, CA. The subject stated that he placed the bomb because he wanted

to kill as many people as he could because Hispanics cost his dad his job and house. The San Jose Police Department's bomb squad was notified and performed a protective sweep of some of the buildings on campus. Nothing was located in the buildings that were searched by officers and K9 officers. An exigent request for subscriber information and location information was sent to Google, LLC for information on the subscriber and location information. An email address of quinnblackbukateferguson1820@gmail.com was provided by Google as the subscriber email, however, there was no location information available.

8. I also noted that on April 25, 2024, at 9:12 a.m., the Carlsbad High School (located at 3557 Monroe Carlsbad, CA 92008) administration office desk phone received an anonymous telephone call threatening a mass shooting. The unidentified male caller stated that he was outside of the school with an AR-15 rifle and was demanding that he immediately be wired $15,000, or else he would enter the campus and begin shooting students. The school was placed on lockdown while the Carlsbad Police Department cleared the campus and surrounding areas. No subjects were located during the search and the school lockdown that was immediately implemented as soon as the phone call was received, was lifted.

9. A few hours later, at 1:40 p.m., a dispatcher from the San Ramon Police Department (SRPD) received a telephone call from a caller that identified himself as DYLAN PIERCE, utilizing telephone number 815-408-0854, who stated that he was calling to report a suspicious person with an AR-15 in front of Ramona High School, located at 1401 Hanson Lane in Ramona, California. The caller stated that the suspicious person was an 18-year old Hispanic male with long hair, glasses, wearing a white shirt and blue jeans. The caller stated that he was sitting in his black Toyota Camry on Ramona Street. The SRPD dispatcher immediately called the San Diego County Sheriff's Department (SDSD) and notified them of the threat and SDSD Deputies responded to the

school. Deputies attempted to locate PIERCE and the described vehicle; however, Deputies were not able to locate either PIERCE or the vehicle. Ramona High School and Olive Pierce middle school were placed on lockdown as a safety precaution. Deputies began to conduct a security sweep of the campus. While conducting a security sweep, at approximately 1:58 p.m., an online suicide hotline service also called the SDSD, and reported that a subject in a suicide chatroom threatened to bomb and commit a mass shooting at Ramona High School. The subject chatted that the bombs would detonate in 45 minutes and he would shoot himself with the firearm he had on his person. The subject identified himself as transgendered, with family issues. Deputies completed the security sweep and did not locate any subjects matching the description or any suspicious objects resembling an explosive device. Ramona High School and Olive Pierce Middle School's lockdown was then lifted.

10. On May 30, 2024, I submitted a Grand Jury Subpoena to Google, LLC, requesting subscriber information on the Google Voice telephone number 815-408-0854 for the timeframe between April 24, 2024 and April 25, 2024. On June 4, 2024, I received the return back from Google, LLC, regarding the request. Google responded that the email address loganclarketour@gmail.com was used as the subscriber email. No other identifying information was provided by Google regarding the subscriber.

11. Given the incidents that occurred between April 24, 2024 through April 25, 2026, utilizing the telephone number 815-408-0854, and the email information provided by Google regarding the subscriber, loganclarketour@gmail.com and quinnblackbukateferguson1820@gmail.com, I am requesting this search warrant in order to obtain information to assist in identifying the individual(s) responsible for the false emergency reporting events.

BACKGROUND CONCERNING GOOGLE

12. In my training and experience, I have learned that Google provides a variety of online services to the public, such as Gmail, Google Voice, various messaging platforms, online wallet services, mapping/navigation services, and more. Google also the owns the Android Operating System software found on upwards of 80% of cellular phones throughout the world. Because of this, Google maintains a plethora of records associated with the various services and software they provide. When registering for many of the various types of Google accounts, Google asks subscribers to provide basic personal information, such as the subscriber's full name, physical address, telephone numbers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Additionally, during the user registration process Google may also record certain identification numbers for the device through which the user accessed Google, such as serial numbers, International Mobile Equipment Identity ("IMEI") numbers, Mobile Equipment Identifier ("MEID") numbers, Electronic Serial Number ("ESN"), etc.

13. Through many of the services offered by Google, a subscriber can store files, address books, contact or buddy lists, calendar data, and pictures on servers maintained and/or owned by Google. Google's email service, called "Gmail," allows users to send and receive electronic messages which are routed through servers maintained and/or owned by Google. The numerous messaging and Voice over Internet Protocol ("VOIP") platforms offered by Google also allow users to communicate with one another by routing conversations through servers maintained and/or owned by Google. These various types of content are often useful in investigations to determine who is using a specific account, who they are communicating with, and the subject of the users' conversations.

14. Aside from content information, Google also records and maintains records of certain types of metadata, such as IP addresses utilized by a user to access Google and geo-location information derived from GPS/cellular signal/Wi-Fi signal/Bluetooth connections of the device through which the user accessed Google. Furthermore, Google keeps records that can reveal Google accounts associated to one another by virtue of the electronic device through which the accounts were accessed, such as the same computer or mobile phone. This includes accounts that are linked by "cookies," which are small pieces of text sent to the user's internet browser when visiting websites. These records, although not personally generated by the user in the way content is created, are a byproduct of the how the services are facilitated and offered by Google.

15. In my training and experience, the types of information maintained by Google may constitute evidence and instrumentalities of the crimes under investigation, and will enable investigators to determine the identities of the unknown actors involved in the blackmail and sextortion scheme of A.Y. as well as other unknown victims. Among other things, the requested information may be relevant in confirming the identities of the users of the Subject Phones and Target Accounts; may assist in the identification of co-conspirators and/or victims; may provide precise location information to determine where the users of the Subject Phones were/are located at the time of communication with the victim; may provide context to the communications on the Subject Phones; and may provide content relevant to the ongoing investigation into potential additional criminal activity committed by the users of the Subject Phones or Target Accounts.

16. The date range for the requested warrants is from July 1, 2023 to October 27, 2023, which is the date range the Google subpoena records show the suspect accounts have been active.

AUTHORIZATION REQUEST

17. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

18. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

19. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

ATTACHMENT A

Property to Be Searched

This warrant applies to information related to the Google accounts associated with the following telephone number and/or email addresses, all of which are stored at premises controlled by Google, Inc. ("Google" or "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043**:**

i. 815-408-0854

ii. quinnblackbukateferguson1820@gmail.com

iii. loganclarketour@gmail.com

.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period April 20, 2024 through April 29, 2024:

1. Subscriber/registration information to include name, emails, phone numbers, addresses, account creation dates, account status, registration IP address, means and source of payment (including any credit or bank account numbers);

2. Device identifiers (IMEI/MEID, serial number, SIM operator, cell operator, and model number, etc.), account identifiers, Android ID, Push Tokens and/or Device Tokens, etc. associated with the Account(s);

3. All IP Address logs for all services utilized by the Account(s), to include records of session times and durations, login/logout/intra-communication IP addresses associated with session times and date, methods of connecting, and log files;

4. Location history for all identified/associated Account(s), to include deleted information, derived from Global Positioning System (GPS) data, cell site/cell tower triangulation precision measurement information such as timing advance or per call measurement data, Wi-Fi location information, and Bluetooth location information. Such data shall include the GPS coordinates, the dates and times of all location recordings, origin of how the location recordings were obtained, and estimated radius;

5. All Gmail address(es) associated with the identified Account(s) including any secondary or backup email addresses associated with the Accounts;

6. The contents of all text messages, voicemails, recorded calls, emails chat messages, and saved drafts associated with the Account(s), including stored/preserved copies and contents maintained on a cloud service, the source and destination addresses associated with each communication, the date and time at which each communication was sent, and the size/length/duration of each communication;

7. All photos and videos stored in the Account(s);

8. Passwords or other protective devices in place and associated with the Account(s), which would permit access to the content stored therein;

9. Web search history, including, but not limited to, mobile and desktop browser searches;

10. Downloaded, installed, and/or purchased apps along with activity/registration information;

11. Voice and/or audio activity recordings/captures;

12. Google Map locations which are saved and/or frequent locations, favorite and/or starred locations including, but not limited to, searches conducted using the Google Map and/or Maze services;

13. Google Voice incoming or outgoing phone calls, voicemails, including voicemail content and any and all incoming or outgoing text message history, together with the content thereof to include SMS, MMS, or any other form of text message communication, and any call forwarding numbers and account backup telephone numbers;

14. Communication including, but not limited to, audio, video, text message and/or chat delivered through the Google, Inc. service known as Google Hangouts;

15. Posts, status updates, photographs and/or videos that are contained and/or were uploaded in the services known as Google Photos, Picasa web albums, Google +, or any other service designed to store video, photographs, and/or data, including the metadata for each file;

16. Electronic files, folders, media, and/or data uploaded and/or contained on the service known as Google Drive;

17. Entries created, deleted, or modified using the service known as Google Keep;

18. Contacts stored using the service known as Google Contacts, including any contacts stored in the service known as Gmail, and any other service where contact lists are maintained;

19. Google Play Store transactions;

20. Additional accounts linked by cookies.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 875, interstate communication with intent to extort.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, Inc. and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, Inc. The attached records consist of _____.

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, Inc., and they were made by Google, Inc. as a regular practice; and

b. such records were generated by Google, Inc.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature